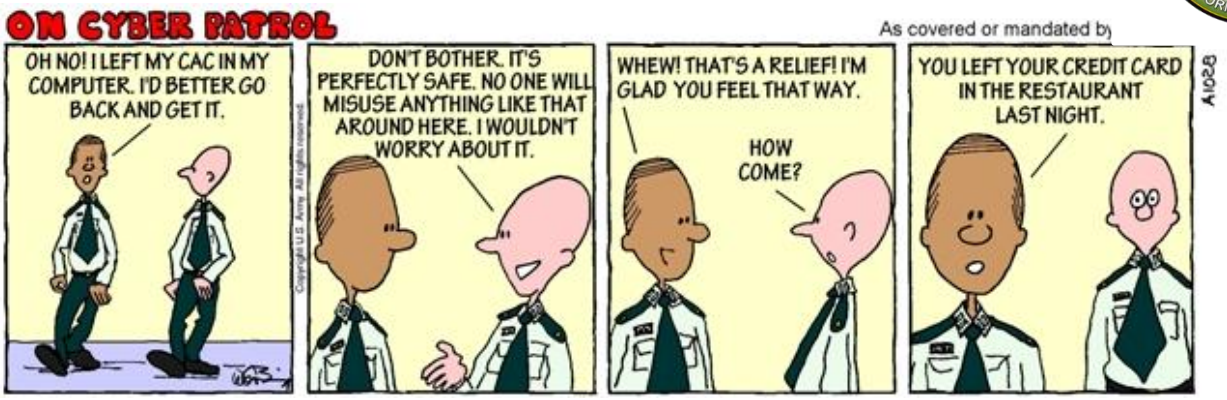
Like Poker- Keep Your Cards Close to Your Chest

August 2007



The following is a briefing from SGT Firewall, Army Cyber Patrol Leader, to a group of Army personnel at a forward camp somewhere in the desert.

As you are aware, your CAC (Common Access Card) is an important security tool to prevent unauthorized access to Army data and systems. It eliminates the necessity for multiple passwords. It also provides a unique user identification that enhances security by granting access to IT systems and resources to only authorized personnel.

Since we have started using CAC, it has made computer use both easier and more secure. Obviously, this is the desired outcome. However, we have noticed that there have been potential security risks because users have not secured their CACs. We have found CACs in computers – still open to secure systems – and in various other places where they shouldn't be. Where they should be is on your person, in a secure location or in your computer with you at the keyboard.

I'm sure all of you have bank cards or credit cards that require a PIN (Personal Identification Number). If you leave them in ATMs the most you lose is a little money that is either limited or covered by the bank. If a bad guy or girl or simply a curious person is able to access a secure Army system because you have left your CAC in your computer, personnel information, operational and other sensitive data can be compromised. If I find your CAC unattended be prepared for some good old fashion push-ups, and lots of them!

So Listen Up: DO NOT LEAVE YOUR CAC UNATTENDED AT ANYTIME! GOT IT? Any Questions?

For more information on the CAC program, visit the Army Information Assurance website: https://informationassurance.us.army.mil/cacpki/ and click on the CAC/PKI Division link or click on the CAC PKI information link on the My Security web page.